ABSTRACT

A method and apparatus for detecting a class of viral code are provided. The apparatus comprises an heuristic analyzer and a search component. The heuristic analyzer heuristically analyzes a subject file and generates a set of flags along with statistical information. The search component uses the set of flags with statistical information to perform a search for a scan string and/or a statement type in the subject file. A positive detection alarm is triggered if the scan string and/or statement type is found at least a corresponding predetermined number of times. The heuristic analyzer may be rule-based and comprise an heuristic engine and heuristic rules. The search component also may be rule-based and comprise a search engine and viral code class rules.